Office Action Summary	Application No.	Applicant(s)	
	10/057,066	XIAO, SIHAI	
	Examiner	Art Unit	
	PONNOREAY PICH	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22,24,29-37 and 50-61* is/are pending in the application.

4a) Of the above claim(s) *7-13 and 31-37* is/are withdrawn from consideration.

5)☒ Claim(s) *22,29 and 30* is/are allowed.

6)☒ Claim(s) *1-6,14-21 and 50-61* is/are rejected.

7)☒ Claim(s) *24* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. *20080424* .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-6, 14-22, 24, 29-30, and 50-61 were examined.

As a preliminary matter, it is noted that the footnotes found on page 12 of the arguments submitted by applicant on 2/5/08 seems to imply that the current application is entitled to an earlier priority date than its actual filing date. The examiner respectfully request clarification on this issue because as noted in the office action mailed on 1/5/06, the examiner found that the priority claim originally made by applicant was erroneous. The response by applicant to the office action mailed on 1/5/06 acknowledged that the current application is not entitled to any priority date. Applicant's latest remarks, however, seems to contradict applicant's earlier confirmation that the current application is not entitled to any priority date.

Response to Arguments

Arguments submitted by applicant on 5/3/08 were fully considered.

Applicant argues that Micali fails to disclose transmitting a TIO to a client. The basis of this argument is that the CIL that the examiner is interpreting as a TIO only discloses whether or not a certificate is issued which is not the same as the trust vector in a TIO which indicates the operations for which the certificate is trusted or not trusted to delegate. First, the examiner respectfully notes that contrary to applicant's argument, the CIL indicates more than just whether or not a certificate is issued. It also indicates whether or not a certificate is valid via a string S (col 7, lines 43-58), which the examiner is interpreting as a trust vector of the CIL/TIO. Further, the examiner respectfully notes that the first limitation recited in independent claims 1, 14, and 22 only refers to the trust

vector of a TIO being indicative of the trust level of trust associated with a particular trust entity certificate. The CIL having an entry that indicates a certificate as valid or not meets the criteria of a trust vector indicating the level of trust associated with a particular trust entity certificate. The second clause of claims 1 and 22 establishes that the trust vector indicates requisite level of trust to establish a connection, i.e. perform a particular operation as applicant is arguing. Claim 14 does not contain a similar limitation as set forth in the second clause of claims 1 and 22. As such, this argument by applicant is found persuasive for claims 1 and 22, but not for claim 14 since claim 14 only requires that a trust vector indicate trust level, not necessarily trust level for a particular operation to be performed as applicant is arguing. As such, the rejections to claims 1 and 22 and their dependent claim are withdrawn based on applicant's argument, but the rejections to claims 14 and its dependent claims are maintained because applicant's argument is not reflective of the limitations that are actually recited in claim 14. Claim 14's trust vector does not require that it indicate a trust level for operations the TIO is trusted or not trusted to delegate.

Applicant argues that Micali fails to disclose verifying a received certificate by determining if it is hashed value corresponds to the one in the TIO and, if so, whether the corresponding trust vector is sufficient for the intended operation--establishing a connection. This argument was found persuasive. As such, the rejections for claims 1 and 22 and their dependent claims are withdrawn also due to this argument being persuasive. This limitation is not found in claim 14, however, thus the rejections for claim 14 and its dependent claims are maintained.

Applicant argues that the combination of Hericourt, Samar, and Micali would not have been obvious. The examiner notes that this argument does not apply to claim 14 and its dependent claims since they were not rejected under the combination of Hericourt, Samar, and Micali. The rejections for claim 14 and its dependent claims are maintained.

Please note new rejections made below based on further search and consideration of the claims.

Claim Objections

Claims 1-3, 22, and 24 are objected to because of the following informalities:

1. "said hash value" recited in claims 1-3 and 22 should be "said plurality of hash values" so as to be consistent with "a plurality of hash values" recited in line 5 of claims 1 and 22 respectively.
2. In claim 24, "said trust entity certificates" in line 5 should be "said plurality of hash values". Note that claim 2 contains a similar limitation where applicant made such a correct already. It is assumed that the correction to claim 24 was overlooked.
3. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 57 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 57 is indefinite because it is unclear, in plain English, what is meant by "said client performs a certificate chain validation up to a root certificate authority (CA)". The support for this claim and the indefinite limitation is found on page 16 of the specification. However, page 16 recites the same thing as what is recited in the claim, thus what is meant by validation up to a root certificate authority is unclear even when the limitation and claim is viewed in light of the specification. It is unclear if applicant is intending to mean that a root certificate authority is somehow used in the certificate chain validation or if applicant meant that certificate chain validation is done up to a certificate belonging to a root certificate authority. A call by the examiner to attorney Frank Carol on 4/23/08 who is assigned to this application, due to Mr. Stephen Driscoll having left the law firm, for guidance on this limitation did not yield any clarification. Mr. Carol stated that the application was in the process of being transferred from his law firm, thus while he was unable to provide clarification, he did forward the examiner's question to the applicant.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-6 and 50-61 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1 is rejected as being directed towards non-statutory subject matter because the steps of the method do not produce a concrete, useful, and tangible result. After all the steps have been performed, it is known whether a trust vector indicates a requisite level of trust to establish a connection. However, merely knowing whether a trust vector indicates a requisite level of trust to establish a connection has no tangibility. It is submitted that if applicant were to add a limitation of establishing a connection if the trust vector indicates a requisite level of trust for the connection, it would overcome this 101 rejection since using the result of the determination to establish a connection is a concrete, useful, and tangible result. Claims 2-6 and 50-61are dependent on claim 1 and also do not produce a concrete, useful, and tangible result, thus are also not statutory.

Claims 14-17 and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hericourt et al (US 2002/0078347) in view of Samar (US 6,304,974).

Claim 14:

Hericourt discloses a TIO (Fig 5), i.e. CAF Table, comprising at least a plurality of hash values, each hash value being hashed from a trusted entity certificate (paragraphs 11, 17, 135 and Fig 4, item 504), and a plurality of trust vectors, each trust vector

corresponding to a hash value and being indicative of the level of trust associated with a particular trusted entity certificate (paragraphs 135 and 138-141 and Fig 4, item 507). *The examiner is interpreting the CAF table as seen in device 308 (see Fig 3) as a TIO. The table contains a plurality of records related to CA certificates. As discussed in paragraphs 11 and 17 a certificate could contain such information as a hash value of the certificate itself. Note that Hericourt does not place any limits on the type of certificates that could be used in his invention. As seen in Figure 5, each record in the table contains the certificate itself, thus the CAF table contains a plurality of hash values hashed from the CA certificate since each certificate contain its own hash. Each record also contains a CA_Trust_Level 507, which the examiner is interpreting as a trust vector. Because there are multiple records, there is a plurality of trust vectors in the CAF table, each vector corresponding to the certificate and hash value.* Hericourt also discloses verifying a received certificate (paragraph 104).

Hericourt does not explicitly disclose of downloading a trust information object (TIO) from a server to said memory of said client. In fact, Hericourt does not discuss at all how device 308 obtained the CAF table, i.e. the TIO. Hericourt discloses that a security administrator periodically maintains the CAF table (paragraph 135). However, because Hericourt does not explicitly explain how the administrator maintains the table one of ordinary skill would recognize that the Hericourt's invention is one which is ready for improvement and one in which one of ordinary skill could apply a variety of known table maintenance techniques to achieve the table maintenance. Samar discloses one manner in which a table is provided to a client is by downloading the table to the client

by an administrator (col 8, lines 20-39). It would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to incorporate Samar's teachings within Hericourt's invention. One skilled would do so by having Hericourt's security administrator create a CAF table and download the table from the administrator's computer, i.e. a server, to a device 308's memory, i.e. a client's memory. The rationale for why it would have been obvious for one of ordinary skill to do this in light of Samar's teachings is that Hericourt's invention is one which is ready for improvement since he does not explicitly teach how a security administrator maintains the CAF table in device 308 and how device 308 obtained the table in the first place. The application of Samar's teachings within Hericourt's invention does no more than yield a predictable result of the security administrator maintaining the CAF table via delivery of the table from a server to a client's memory, i.e. delivery from the administrator's computer to device 308's memory.

As per the limitations of said client periodically connecting to said server to determine whether a new TIO is available; and said server sending a new to said client if said new TIO is available, the limitations are disclosed by Samar (col 8, lines 20-44), thus are obvious to Hericourt and Samar's combination invention.

Claim 15:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Further, Samar discloses sending said TIO with a signing certificate to said client, wherein trust information of said signing certificates indicates that said signing certificate can be trusted for signing said TIO (col 3, lines 4-13).

Claim 16:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Samar further discloses wherein said client fetches said TIO from a trusted server, said client ensuring that a root certificate that signed said signing certificate is contained in said TIO (Fig 5).

Samar does not disclose said root certificate is not revocable. However, the examiner asserts that non-revocable certificates were well known in the art at the time applicant's invention was made. It would have been obvious to one of ordinary skill in the art to further modify Hericourt's invention such that the root certificate was not revocable because it would indicate a high level of trust for the user of the root certificate.

Claim 17:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Samar further discloses wherein said client verifies a digital signature of said TIO with a signing certificate, along with a TIO sent to said client (col 5, lines 46-51 and col 7, lines 17-23).

Claim 20:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Hericourt does not explicitly disclose wherein said TIO is delivered to said client via a broadcast channel; wherein a provider delivers an initial TIO to said client that contains a signing certificate and associated trust information by either of including said signing

certificate in the initial TIO saved in a client persistent memory, or by sending the initial TIO to said client through a secure channel before using said broadcast channel.

However, the examiner asserts that the limitation is well known in the art, as discussed in a prior office action. At the time applicant's invention was made, it would have been obvious to one of ordinary skill to further modify Hericourt's invention to use a broadcast channel as recited in claim 20. One skilled would have been motivated to do so because sending a TIO via a broadcast channel is the quickest and cheapest way of distributing the same information to a large group of clients. One of ordinary skill would have been motivated to deliver an initial TIO to the client via a secure channel before using a broadcast channel as this would initially ensure that only authorized clients received subsequent TIO's.

Claim 21:

Hericourt and Samar renders obvious all the limitations recited in claim 14. Hericourt does not explicitly disclose updating said TIO on a per session basis when said TIO is not persistently stored. However, as discussed in the prior office action, this limitation was well known in the art at the time applicant's invention was made. It would have been obvious to one skilled to have further modified Hericourt's invention according to the limitations recited in claim 21. One skilled would have been motivated to do so because it would prevent untrustworthy certificates from being used.

Claims 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hericourt et al (US 2002/0078347) in view of Samar (US 6,304,974) and further in view of Vogel et al (US 6,816,900).

Claim 18:

Hericourt and Samar renders obvious all the limitations recited in claim 17. Hericourt does not explicitly disclose wherein multiple signatures are verified, depending on the number of signatures specified in said TIO; wherein said client hashes said signing certificates one by one; and wherein if proper results are found in said TIO and said certificates are trusted for signing said TIO, then said TIO proves that it was not tampered with.

However, Vogel discloses wherein multiple signatures are verified, depending on the number of signatures specified in a TIO (col 8, lines 9-17). Vogel also does not explicitly disclose wherein if proper results are found in said TIO and said certificates are trusted for signing said TIO, then said TIO proves that it was not tampered with. However, the purposes of signatures are to verify and validate. If proper results are found for the signatures, then by definition, the TIO has proven that it was not tampered with.

It would have been obvious to one of ordinary skill to further modify Hericourt's invention according to the limitation recited in claim 18 in light of Vogel's teachings because it would allow one to determine which CA's are no longer trustworthy due to possible security breaches. Note Hericourt discloses wanting to remove untrustworthy CA's from the list of trusted CA's (paragraphs 136-137).

Claim 19:

Hericourt and Samar renders obvious all the limitations recited in claim 19. Hericourt does not explicitly disclose wherein said signing certificates exist in said TIO in said client before said TIO is signed. However, official notice is taken that at the time applicant's invention was made, it was well known for a client to receive and store a signing certificate from a CA before messages signed with the certificate is sent to the client. In light of this, it would have been obvious for one skilled to have further modify Hericourt's invention according to the limitations recited in claim 19. One skilled would have been motivated to do so because it would allow a client to quickly verify the authenticity of a message/response/TIO received if the client already had the signing certificate with which it can perform authentication of a signature.

Allowable Subject Matter

Claims 1-6 and 50-61 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 101, any rejection(s) under 35 U.S.C 112, 2nd paragraph, and any objections set forth in this Office action.

Claims 22, 24, and 29-30 would be allowable if rewritten or amended to overcome any objections set forth in this Office action.

These claims are considered to contain allowable subject matter over the prior art because as discussed above, applicant's arguments were considered persuasive with respect to these claims. The prior art does not teach a TIO having trust vectors, wherein a trust vector indicates a requisite level of trust to establish connection. The prior art also does not teach if a match of a resulting hash value is found in a TIO,

determining if the corresponding trust vector indicates requisite level of trust to establish connection as required by the second limitation recited in claims 1 and 22.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PONNOREAY PICH whose telephone number is (571)272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Examiner, Art Unit 2135